معارف
ISSN 1112-7007
EISSN 6804 -2600
المجلد 18/ العدد 1 (جوان 2023): ص.ص:1092-1111

# الجرائم السيبرانية في الفضاء الاتصالي الجزائري: أنواعها، آثارها وسبل مواجهتها

# Cybercrime in the Algerian communication space: types, effects and means of confrontation

نسيمة مقبل*

كلية علوم الإعلام والاتصال، جامعة الجزائر 3، الجزائر، nassmekbel@yahoo.fr

تاريخ الاستلام: 2022/02/21؛ تاريخ القبول: 2023/04/02؛ تاريخ النشر: 2023/06/05

**ملخص:**

تطرح الجرائم السيبرانية بمختلف أشكالها نقاشا واسعا في الفضاء الأكاديمي والقانوني وهذا نظرا لآثارها الوخيمة على الفرد والمؤسسات والدول، ومن أجل مواجهتها والتقليل من تداعياتها عمدت الجزائر على غرار بقية بلدان العالم على وضع قوانين خاصة لتنظيم الأنشطة الاتصالية في الفضاء السيبراني وتجنب كل المخالفات والتجاوزات التي تصب في إطار الجريمة السيبرانية. وعليه جاءت هذه الورقة البحثية لترصد واقع الجرائم الإلكترونية في التشريع الجزائري ومدى اهتمام هذا الأخير بمواجهة الظواهر السلبية التي يشهدها الفضاء الإلكتروني ومدى جدية وشمولية المواد القانونية ووضوحها ومصادر التشريع فيما يتعلق بتبيان طبيعة الجريمة وحدودها والعقوبة المفروضة والتفريق بين الجريمة السيبرانية وحرية التعبير والحق في الإعلام والحق في الاتصال، ومن أجل هذا اعتمدنا في هذه الدراسة على المنهج المسحي الوصفي لهذه الظاهرة مع توظيف أداة الملاحظة العلمية والتحليل لمختلف المواد القانونية المخصصة للجريمة السيبرانية.

**كلمات مفتاحية:** فضاء إلكتروني؛ جريمة سيبرانية؛ تشريع جزائري.

**Abstract:**

Cybercrime in its various forms raises a wide debate in the academic and legal space, due to its dire effects on the individual, institutions and countries. In order to confront it and reduce its repercussions, Algeria, like the rest of the world, set out special laws to

* المؤلف المرسل.

regulate communication activities in cyberspace and avoid all violations and abuses that fall within the framework of cybercrime.

Accordingly, this research paper came to monitor the reality of cybercrime in Algerian legislation, the extent of the latter's interest in confronting the negative phenomena witnessed by cyberspace, the seriousness and comprehensiveness of the legal articles and their clarity, and the sources of legislation with regard to clarifying the nature of the crime, its limits, the penalty imposed, and the distinction between cybercrime and freedom of expression and the right to information and the right to freedom of expression. Connection.

For this reason, in this study, we relied on the descriptive survey approach for this phenomenon, while employing the scientific observation and analysis tool for the various legal materials devoted to cybercrime.
**Keywords:** Cyberspace; cybercrime; Algerian legislation .

## المقدمة:

سارعت العديد من الدول منذ نهاية القرن الماضي لإيجاد تشريعات خاصة قصد مكافحة الجرائم السيبرانية، وبكونها جرائم عابرة للقارات صدرت اتفاقية بودابيست سنة 2001 المتعلقة بهذا النوع من الجرائم، والتي تهدف إلى تعزيز التعاون الدولي والإقليمي لدرء مخاطر هذه الجرائم.

فغالبا ما يترتب عن الجريمة السيبرانية ضرر جسيم للأفراد أو المؤسسات، ويكون في أغلب الأحيان الدافع من وراء ارتكابها ابتزاز الضحية وتشويه سمعتها من أجل تحقيق مكاسب مادية وذلك باستخدام الحاسوب ووسائل الاتصال الحديثة مثل الإنترنت.

تتشابه الجريمة السيبرانية مع الجريمة العادية في عناصرها من حيث وجود الجاني والضحية وفعل الجريمة، ولكن تختلف عن الجريمة العادية باختلاف البيئات والوسائل المستخدمة، فالجريمة الإلكترونية يمكن أن تتم دون وجود الشخص مرتكب الجريمة في مكان الحدث، كما أن الوسيلة المستخدمة هي التكنولوجيا الحديثة ووسائل الاتصال الحديثة والشبكات المعلوماتية.

ما من شك اليوم أن الجزائر تأخرت في وضع قانون لمكافحة الجرائم الإلكترونية، خاصة وأن أغلب الدول المتقدمة سنّت قوانين في الغرض منذ أواخر القرن الماضي وذلك لوعيها بتداعيات هذه الجرائم على سلامة الأفراد والدولة.

وتحرص الدول الديموقراطية عند سنّ القوانين المقيّدة للحقوق والحريات على استعمال أقل الوسائل تدخلا لعدم إلغاء الحق، كما غالبا ما يتمتع القضاة بسلطة واسعة بغاية الدفاع عن الحريات. إلا أن الأنظمة الدكتاتورية تتخذ من قوانين مكافحة الجريمة السيبرانية مثلا غطاء لإلغاء حقوق أخرى على غرار الحق في الخصوصية والحق في حريّة التعبير دون تهديد أو ترويع.

وعليه سنحاول من خلال هذه الورقة البحثية أن نتطرق إلى نظرة المشرع الجزائري لظاهرة الجريمة الإلكترونية وكيفية التعامل القانوني معها ومدى ملائمة النصوص القانونية للتطور الكبير الذي يشهده الفضاء السيبراني . وعليه نطرح السؤال الجوهري التالي: **كيف أثرت الجرائم السيبرانية على الفضاء الاتصالي الجزائري ؟**

ومن أجل الإجابة عن سؤال الإشكالية نقوم بتفكيكها إلى جملة من التساؤلات الفرعية التي تنطوي تحتها أهداف الدراسة كما يلي:

- ما هو مفهوم الجريمة السيبرانية ؟
- ما هي خصائص الجريمة السيبرانية ؟
- ما هي أنواع الجرائم السيبرانية ؟
- ما هي أهم القوانين التي تطرقت إلى الجرائم السيبرانية ؟

وتبرز أهمية هذه الدراسة فيما يلي:

-يعتبر مفهوم الجريمة السيبرانية في التشريع الجزائري ضمن المفاهيم الجديدة للظاهرة الاتصالية، ويعتبر مدخلا إضافيا لرصد التطورات في مجال استخدام الفضاء السيبراني -تعتبر الدراسة إسهاما في مناقشة موضوع هام جدا لم ينل حقه في المناقشة والتحليل في الدراسات العلمية بالشكل الكافي.

- تعد الدراسة مرجعا في بناء أسس الاستخدام السليم والعقلاني لتطبيقات الفضاء السيبراني من أجل الاستفادة من المزايا التفاعلية في تسهيل الخدمات بدون مخالفات.

تتمثل المنهجية المتبعة في هذه الدراسة في استخدام أساليب منهجية فرضتها أهمية

الدراسة والهدف العام لها، كما فرضتها معالجة ومناقشة ثم تحليل موضوع الجريمة السيبرانية في الفضاء الاتصالي الجزائري، مما يستدعي ضرورة اختيار طريقة البحث وأدواتها المناسبة التي تثيرهما المشكلة وهي:

أسلوب المسح "الذي يعتبر من أبرز الأساليب المنهجية في مجال الدراسات الإعلامية، والذي يمثل جهدا علميا منظما للحصول على بيانات ومعلومات حول الظاهرة أو مجموعة من الظواهر موضوع البحث .

كما يستفاد من هذا الأسلوب المنهجي في دراسة الإشكالية وتفكيكها إلى عناصرها التراتبية، بغية التوصل إلى دلالات مفيدة.

وانطلاقا من ذلك لجأت الباحثة إلى الاستعانة بالتحليل والتفسير، للخروج باستنتاجات منطقية قصد الإجابة عن تساؤلات الدراسة.

ومن خلال هذه الدراسة أردنا معرفة العلاقة التي تربط الجريمة السيبرانية كظاهرة اتصالية والتشريع الجزائري كواجهة قانونية رادعة وإبراز كيفية تعامله مع هذه الجرائم وطبيعة العقوبات المفروضة على المجرم السيبراني .

وبالنسبة للأدوات المستعملة، فقد قامت الباحثة بعرض الإسهامات البحثية المتصلة بالجرائم السيبرانية، من حيث المفهوم، الخصائص، السمات، الأنواع، الفوائد والأضرار استنادا إلى تساؤلات الدراسة، وباستخدام أداة الملاحظة، ثم التمحيص والتحليل لاستخراج النتائج.

بناءً على ذلك يتسنى لنا معالجة المحاور الأساسية التي يتألف منها الموضوع المطروح للمعالجة على النحو الآتي:

## المحور الأول: مدخل مفاهيمي إلى الجريمة السيبرانية

### 1.تعريف الجريمة السيبرانية

الجريمة السيبرانية هي: "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي، أو هي مختلف صور السلوك الإجرامي التي ترتكب باستخدام المعالجة الآلية للبيانات .

ويرى الأستاذ MASS أن المقصود بالجريمة الإلكترونية: "الاعتداءات القانونية التي

ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"[1].

كما أن مجرد استخدام الحاسب الآلي لا يضيف إلى السلوك غير المشروع جديدا، ولكن استخدام البيانات والمعلومات والبرامج هو الذي يمكن أن يضيف إلى الجريمة سمة الجريمة السيبرانية.

وجل هذه التعريفات تعرضت للنقد من قبل الفقه، لذلك حاول جانب آخر من الفقه تعريف الجريمة السيبرانية على نحو واسع من أجل محاولة تفادي أوجه القصور التي شابت تعريفات الاتجاه المضيق في التصدي لظاهرة الإجرام المعلوماتي.

من بين التعريفات الموسعة للجريمة السيبرانية ما ذهب إليه من الفقه الأستاذ هلالي عبد الله أحمد بقوله: " عمل أو امتناع عن عمل يأتيه الإنسان إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض للاعتداء عليها عقابا"

ويمتاز هذا التعريف بالمزايا التالية :

- أنه يحتوي على كل صور الاعتداء الإيجابية أو السلبية التي توقع أضرار بمكونات الحاسب المادية أو المعنوية.
- أنه يتضمن الأثر الجنائي المترتب على العمل أو الامتناع غير المشروعين والذي يتمثل في الجزاء الجنائي بشتى صوره وأنواعه.
- يحافظ على الشرعية الجنائية: "لا جريمة ولا عقوبة أو تدبير أمن بغير قانون"

و نظرا لخطورة هذه الجريمة وآثارها الممتدة التي قد تصل من دولة لأخرى، فإن بعض الهيئات الدولية المعنية بجرائم الكمبيوتر قد أرست قواعد لتعريف هذا النوع من الجرائم، من هذه الهيئات الـOECD ، التي اتخذت التعريف التالي كتعريف لجريمة الكمبيوتر بأنها: " أي سلوك غير قانوني أو غير قانوني أو غير أخلاقي أو غير مفوض يتعلق بالنقل أو المعالجة الآلية للبيانات يعتبر اعتداءً على الكمبيوتر"[2].

بعد التطرق إلى تعريف الجرائم الإلكترونية التي تعد إفرازا ونتاجا لتقنية المعلومات نخوض في البحث عن خصائص هذه الجريمة التي تميزها عن غيرها من الجرائم التقليدية

(1)عبير شفيق الرحباني، **الجرائم الإلكترونية ومخاطرها**، دار الثقافة للنشر والتوزيع، الأردن، 2020، ص 18 .

(2)محمود عمر محمود ، **الجرائم المعلوماتية والإلكترونية بالتطبيق على الهاتف المحمول**، خوارزم العلمية، السعودية، 2015، ص 34 .

أو المستحدثة بمجموعة من السمات قد يتطابق بعضها مع صفات أنواع أخرى من الجرائم هذا من ناحية، ومن ناحية أخرى فإن اختلاف الجرائم الإلكترونية عن الجرائم التقليدية من حيث الأفعال الإجرامية أكسبها خصوصية غير عادية.

## 2.خصائص الجريمة السيبرانية:

يصعب متابعة جرائم الحاسب الآلي والإنترنت وكذا الكشف عنها، لأن هذه الجرائم لا تترك أثرا فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تتغير في السجلات ومعظم جرائم الحاسب الآلي تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أن الجرائم للتي لم تكتشف هي أكثر بكثير من تلك التي كشف الشر عنها، وتعود أسباب صعوبة إثبات هذا النوع من الجرائم إلى الأمور التالية[1] :

- أنها كجريمة لا تترك أثرا بعد ارتكابها ويصعب الاحتفاظ بأثرها إن وجدت .
- تحتاج غلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها.
- أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبها.

بالإضافة إلى أن ارتباط الجريمة السيبرانية بجهاز الحاسب الآلي وشبكة الإنترنت أضفى عليها مجموعة من الخصائص التي تميزها عن الجرائم التقليدية، ولعل من أهمها ما يلي[2] :

- **الخاصية الأولى:** جرائم الحاسوب ترتكب بواسطة الحاسب الآلي وكذلك عبر شبكة الإنترنت فهي حلقة الوصل الرئيسية بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك والشركات وغيرها من الأهداف التي تكون غالبا الضحية لتلك الجرائم .

- **الخاصية الثانية:** أنها جريمة عابرة للحدود، فالمجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود، وهو خلق العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة وكذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى شكليات تتعلق بإجراءات الملاحقة القضائية وغيرها من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.

(1)عبير شفيق الرحباني، مرجع سبق ذكره، ص 27 .

(2)محمد عبد الرحمن عنانزة، **القصد الجرمي في الجرائم الالكترونية**، دار الأيام للنشر، عمان، 2017، ص51.

- **الخاصية الثالثة:** صعوبة التحري والتحقيق نظرا لارتكابها في الخفاء، وعدم وجود أي أثر إيجابي لما يجري خلال تنفيذها من أفعال إجرامية، فالتحري عنها ينطوي على العديد من المشكلات والتحديات الإدارية والقانونية، والتي تتصل ابتداءً من عملية ملاحقة الجناة، فإذا تحققت إمكانية الملاحقة أصبحت الإدانة صعبة لسهولة إتلاف الأدلة من قبل الجناة أو لصعوبة الوصول إلى الأدلة أو لغياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجريمة.

- **الخاصية الرابعة:** تتسم بالخطورة البالغة من عدة جوانب، فمن ناحية أولى نجد الخسائر الناجمة عنها كبيرة جدا قياسا بالجرائم التقليدية خاصة جرائم الأموال، ومن ناحية ثانية نجدها ترتكب من فئات متعددة تجعل من التنبؤ بالمشيئة فيه أمرا صعبا ومن ناحية ثالثة تنطوي على سلوكيات غير مألوفة.

ولا أدل على ذلك من أن الخسائر المادية الناجمة عن هذه الجرائم تبلغ وفقا لتقديرات المركز الوطني لجرائم الحاسب في الولايات المتحدة الأمريكية في نهاية القرن الماضي حوالي 500 مليون دولار في السنة، وذلك في نهاية القرن العشرين .

- **الخاصية الخامسة:** الصورة التقليدية للمجرم تكاد تختفي في هاته الجرائم بل وعلى العكس من ذلك فالمجرم المعلوماتي عادة ما ينتمي إلى مستوى اجتماعي مرتفع عن غيره من المجرمين ونادرا ما يكون محترفا للإجرام أو عائدا، كما أنه لا ينظر إليه كمجرم بالمعنى المتعارف عليه لهذه الكلمة وذلك لكون الأسباب والعوامل التي تقف وراء ارتكاب الجريمة المعلوماتية تختلف بالمقارنة بالجريمة التقليدية.

- **الخاصية السادسة:** قلة الإبلاغ عن وقوع الجريمة المعلوماتية، وذلك راجع لسببين أولهما الخشية والخوف من التشهير، لذلك نجد أن معظم جرائم الإنترنت تم الكشف عنها بالصدفة أو بعد فترة طويلة من ارتكابها، والسبب الثاني هو عدم اكتشاف الضحية للجريمة مما يعني أن الجرائم التي حدثت ولم يتم اكتشافها هي أكثر بكثير من الجرائم التي تم كشف الستار عنها .[1]

وعليه فالجريمة السيبرانية تعتبر من أحدث أنواع الجرائم، مسرحها العالم الافتراضي

(1)محمد عبد الرحمن عنانزة، مرجع سبق ذكره، ص 53 .

غير ملموس بعيدة عن أي مظهر من مظاهر الجريمة التقليدية فهي جريمة عابرة للحدود يرتكبها مجرمون ذو مستوى عالي، أذكياء ومتميزون في المجال التقني، مما يؤدي إلى تشتيت الجهود الدولية في محاولة تعقبها التحري عنها، أو الوصول إلى مرتكبها.

وقد صنف الفقهاء والدارسون جرائم الكمبيوتر والإنترنت ضمن فئات متعددة تختلف حسب الأساس والمعيار الذي يستند إليه التقسيم المعني، وهذا ما سنتعرض إليه فيما يلي.

### 3.تصنيف الجرائم السيبرانية :

يصعب تصنيف الجرائم نظرا لاختلافها من مجتمع لآخر من حيث تطوره، ومدى استخدامه للحاسوب ودرجة اعتماده عليه في مختلف جوانب الحياة، وقد أوجد مشروع اتفاقية جرائم الكمبيوتر والإنترنت لعام 2001 (اتفاقية بودابست 2001) تضمن أربع طوائف رئيسية[1] :

**أ.الجرائم التي تستهدف سلامة وسرية المعطيات والنظم:** وتضم الدخول غير قانوني (غير مصرح به )، الاعتراض غير القانوني، تدمير المعطيات، اعتراض النظم.

**ب. الجرائم المرتبطة بالكمبيوتر:** تضم التزوير المرتبط بالكمبيوتر، الاحتيال المرتبط بالكمبيوتر.

**ج. الجرائم المرتبطة بالمحتوى:** وهي تضم طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعقلة بالأفعال الإباحية واللا أخلاقية .

**د.الجرائم المرتبطة بالأشخاص والأموال:** وتضم السرقة والاحتيال والتزوير والاطلاع على البيانات الشخصية، المعلومات المضللة والزائفة، أنشطة الاعتداء على الخصوصية إساءة استخدام المعلومات، القرصنة ... وغيرها من الجرائم.

وعليه، فقد تعدد الجهود الفقهية التي بذلت على الصعيد الدولي أو الوطني من أجل وضع تقسيم يمكن الاعتماد عليه لجرائم المعلوماتية، وفي هذا المجال يمكن تقسيمها إلى مجموعتين أساسيتين :

**المجموعة الأولى:** الجرائم التي تقع على الإنترنت أي أن الشبكة العنكبوتية تكون عنصر

(1) Thomas J. Holt, **Cybercrime and Digital Forensics An Introduction**, Routledge, USA , 2022, p 71 .

سلبي في الجريمة أي محل للجريمة فقط، فإن هدف المجرم ينصب حول البيانات والمعلومات المخزنة والمنقولة عبر قنوات الخاصة أو العامة واختراق الحواجز الأمنية إن وجدت والاعتداء على الأموال، والتي نذكرها على التوالي.

**أ. سرقة المال المعلوماتي** :أضحى لبرامج المعلومات قيمة غير تقليدية لاستخداماتها المتعددة في كافة المجالات الاجتماعية والاقتصادية فهذه القيمة المميزة لبرامج المعلومات تجعلها محلا للتداول، وهنا تبدو أهمية الإنترنت بصفته مصدر المعلوماتية، مما أدى إلى ظهور قيمة اقتصادية جديدة وأموال جديدة، عرفت بالأموال المعلوماتية، وصاحب ظهور هذا المال المعلوماتي جرائم جديدة عرفت بالجرائم المعلوماتية وهذه الجرائم يمكن تصورها من زاويتين :

أن تكون المعلوماتية أداة أو وسيلة للاعتداء، وأن تكون المعلوماتية موضوعا للاعتداء رأي سرقة تلك المعلومات.

فالزاوية الأولى يستخدم الجاني المعلوماتية لتنفيذ جرائم سواء ما تعلق منها بجرائم للاعتداء على الأشخاص أو الأموال كالسرقة والنصب وخيانة الأمانة، أما الجرائم من الزاوية الثانية يكون المال المعلوماتي موضوعا لها.

**ب. استخدام البروكسي للدخول إلى المو اقع المحجوبة** :هو عبارة عن برامج وسيط يقوم بحصر ارتباط جميع مستخدمي الإنترنت في جهة واحدة ضمن جهاز موحد وهذا البرنامج يستخدم لتجاوز المواقع المحجوبة، والتي عادة ما تكون إما مواقع جنسية أو سياسية معادية للدولة .

**ج . جرائم الاختراق** :يمثل الاختراق المعلوماتي تحديا على قدر كبير من الأهمية لإنجازات تكنولوجيا المعلومات، ويعرفه شراح القانون المعاصرون بأنه: " فعل مشروع يوظف المعرفة العلمية السائدة في ميدان ثقافة الحاسوب والمعلوماتية لاقتراف إساءة أو هجوم على الغير.

فهي عملية اقتحام الأنظمة أو الشبكات الخاصة بأفراد أو منظمات خاصة أو حكومية بمساعدة بعض البرامج المتخصصة في فك وسرقة كلمات السر، يقوم المستخدمون المخولون بفتح حسابات الشركات أو المؤسسات للأغراض الشرعية مثل اللعب بالحسابات

الشخصية ومزاولة بعض أنواع الألعاب في الحاسوب للوصول إلى الأسرار الخاصة بالمؤسسة عن طريق كسر كلمات السر الخاصة بالأنظمة خلال خطوط شبكات الهاتف .[1]

وفيها تعرض بعض الأساليب المستخدمة في عمليات الاختراق :

.الاقتحام أو التسلسل.

.الفيروسات.

**د . المو اقع المعادية** :بعض المواقع يتم إنشائها لمعاداة سياسية أو معاداة الدين أو للأشخاص أو الجهات.

**هـ . جر ائم القرصنة** :تواجه شبكة الإنترنت ما يسمى بظاهرة القرصنة، والتي تكون من قبل بعض الجماعات التي تؤمن بالحرية المطلقة في الرأي والتعبير والاستخدام أيضا، وهي جماعات تستطيع أن تدخل عبر طرق خاصة تحترق أجهزة الحاسوب، وكذا الأرقام السرية للأشخاص وإلى بريدهم الإلكتروني.

فهي تعتبر سرقة للخدمات أو الاستعمال غير المصرح به للنظام المعلوماتي .

**و.جر ائم التجسس الإلكتروني :**

هي الجرائم التي يتم بواسطتها اختراق أجهزة المستخدمين بطرق غير شرعية ولأغراض غير سوية، من أجل سرقة المعلومات تتعلق بذلك المستخدم سواء على الصعيد الشخصي، أو السياسي أو العلمي أو الاجتماعي حيث لم يعد هناك سرية يمكن الاحتفاظ بها من دون أن يقوم الشخص بعمليات كثيرة لتجنب عمليات التجسس أو "الهاكرز."

فهي ممارسات غير مشروعة على شبكات الحاسب الآلي، تستهدف التحاليل على نظام المعالجة الآلية للبيانات بغية إتلاف المستندات المعالجة إلكترونيا.

**ي . الإرهاب الإلكتروني :**

يعد الإرهاب المعلوماتي من أخطر أصناف الجرائم المرتبطة بتكنولوجيا المعلوماتية نظرا لأثرها ودوافعها فالإرهاب الإلكتروني هو تحطيم أو إتلاف أنظمة معلوماتية بهدف المساس، أو إحداث خلل يمس باستقرار دولة أو بهدف الضغط على حكومة ما .

(1) Thomas J. Holt , op.cit , p 75 .

فهو هجوم مع سبق الإصرار، ذو أهداف سياسية ضد المعلوماتية، ضد أهداف مسلحة (الشرطة، الدرك أو أهداف عسكرية)، أو غير مسلحة (كالإدارات المدنية الوطنية)، من طرف جماعات وطنية أو خفية.

وخطورة الإرهاب الإلكتروني تزداد في الدول المتقدمة التي تضار بنيتها التحتية بالحواسيب الآلية والشبكات المعلوماتية، مما يجعلها هدفا سهل المنال فبدلا من استخدام المتفجرات تستطيع الجماعات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية وإغلاق المواقع الجوية وشل أنظمة القيادة.

## المحور الثاني: الجريمة السيبرانية في القوانين الجزائرية

سعيا من المشرع الجزائري في التصدي لظاهرة الإجرام السيبراني وما يصاحبها من أضرار معتبرة على الأفراد وعلى مؤسسات الدولة من جهة، ومحاولة منه تدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى، عمد منذ الألفية الثانية إلى تعديل العديد من القوانين الوطنية بما فيها التشريعات العقابية على رأسها قانون العقوبات لجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجية الإعلام والاتصال، وقام باستحداث قوانين أخرى خاصة لضمان الحماية الجنائية للمعاملات الإلكترونية .

قد أخص المشرع الجزائري تنظيم الجريمة السيبرانية بقوانين عامة وأخرى خاصة وهذا ما سنتطرق إليه فيما يلي:

### 1. الجريمة السيبرانية في قانون العقوبات:

لقد تعرض المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي في قانون العقوبات بموجب القانون 15/04 تحت عنوان: "المساس بأنظمة المعالجة الآلية للمعطيات" ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 مكرر 8[1].

و في عام 2006 أدرج المشرع تعديل آخر على قانون العقوبات بموجب القانون 23/06 حيث مس هذا التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال.

(1) القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات، ج.ر .عدد 71.

ويرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى.

أما بالنسبة لأنواع الجرائم الإلكترونية المنصوص عليها في قانون العقوبات والتي يمكن تصنيفها إلى ما يلي[1] :

- الغش أو الشروع فيه، في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات.
- حذف أو تغيير لمعطيات المنظمة.
- إدخال أو تعديل في نظام المعطيات.
- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار.
- حيازة أو إفشاء أو نشر أو استعمال المعطيات.
- تكوين جمعية الأشرار.

وعليه، يمكن تكييف هذه الأفعال الإجرامية بأنها جرائم ضد أموال الغير والمضرة بالمجتمع.

وتجدر الإشارة إلى أن المشرع قد قام بتعديل قانون العقوبات في سنة 2016، مستحدثا بذلك نصا جديدا وهو المادة 87 مكرر 12 والتي أحدثت لنا جريمة جديدة وهي جناية تجنيد الأشخاص لصالح إرهابي أو منظومة إرهابية باستخدام وسائل تكنولوجيا الإعلام والاتصال[2].

وصرحت المادة 12: لا يُعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات.

وفي المادة 40: حيث تضمن الدولة، عدم انتهاك حرمة الإنسان. ويحضر أي عنف بدني أو معنوي أو أي مساس بالكرامة. المعاملة القاسية أو اللاإنسانية أو المهينة يقمعها القانون.

أيضًا تنص المادة 303 من قانون العقوبات على يعاقب بالحبس من ستة أشهر إلى ثلاث

(1) القانون رقم 23/06 المؤرخ في 20 ديسمبر المعدل والمتمم لقانون العقوبات، ج.ر .عدد 84.

(2) القانون رقم 02/16 المؤرخ في 19 ماي 2016 المعدل والمتمم لقانون العقوبات، ج.ر .عدد 37.

وبغرامة من 50.000 دج إلى 300.000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص.

ويكون هذا المساس بأكثر من طريقة أو تقنية سواء للصور الشخصية أو المحادثات، وسواء الارتكاب الفعلي أو مجرد الشروع فيه، بالعقوبات ذاتها المقررة للجريمة التامة.

فالمادة 287 من قانون العقوبات تنص على يعاقب بالحبس من ثلاث أشهر إلى سنة، وغرامة مالية من 20.000 إلى 100.000 دج، إذا كان التهديد بالعنف أو القتل.

أما إن كان مصحوبا بأمر أو شرط شفهي أي عقوبة تشويه السمعة في القانون الجزائري فيعاقب الجاني بالحبس من ستة أشهر إلى سنتين، وبغرامة من 20.000 إلى 100.000 دج.

## 2. الجريمة السيبرانية في قانون الإجراءات الجزائية:

فيما يتعلق بمتابعة الجريمة الإلكترونية فهي تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية كالتفتيش والمعاينة، واستجواب المتهم والضبط والتسرب والشهادة والخبرة . غير أن المشرع الجزائري فقد نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية .

كما نص على التفتيش في المادة 45 الفقرة 7 من نفس القانون المعدلة حيث اعتبر أن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد العامة من حيث الشروط الشكلية والموضوعية[1].

ونص كذلك المشرع على التوقيف للنظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6 وكذالك على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

أما بالنسبة لباقي الإجراءات من تحقيق ومحاكمة فإنه تطبق عليه نفس إجراءات الجريمة التقليدية.

(1) المادة 45 من القانون رقم 07/17 المؤرخ في 27 مارس 2017 المعدل والمتمم لقانون الإجراءات الجزائية، ج.ر .عدد 20.

### 3.الجريمة السيبرانية في القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

يهدف هذا القانون إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

وقد تبنى هذا القانون تعريف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وكل ما يتعلق بالمنظومة المعلوماتية وكذا معطيات المعلومات ومقدمو الخدمات .

وقد خول هذا القانون بعض الإجراءات التي تطبق على الجرائم السيبرانية من[1] :

- مراقبة الاتصالات الإلكترونية.
- تفتيش المنظومة المعلوماتية.
- حجز المعطيات المعلوماتية.

وقد أنشأ بموجب هذا القانون هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والتي من مهامها :

- تفعيل التعاون القضائي والأمني وإدارة وتنسيق العمليات الوقائية.
- تبادل المعلومات مع الجهات الأجنبية من أجل تفعيل الحماية على المنظومة المعلوماتية من كل خطر يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

وقال وزير العدل عبد الرشيد طبي على هامش اليوم الدراسي حول "دور التشريع والفقه والاجتهاد القضائي في تطوير القانون" المنعقد في قاعة المحاضرات بمجلس الدولة، "إن الاجتهاد القضائي هو منبع للقانون فالقضاة عادة ما يستأنسون بالآراء الفقهية في المسائل الشائكة التي تعرض عليهم[2]."

"فقد حدث تعديل لقانون الإجراءات الجزائية، حيث تم إنشاء القطب الوطني

(1) القانون رقم 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، ج.ر .عدد 47.

**(2)**علي ياحي ( 2022/03/07)، **تطوير المنظومة القضائية والأمنية في الجزائر لمواجهة الجرائم المعلوماتية**، https://www.independentarabia.com/node/309351/، تم الإطلاع عليه بتاريخ 2022/11/07 .

المتخصص في محاربة الجريمة الإلكترونية وتشديد العقوبات على بعض الجرائم الإلكترونية"، مؤكدا أنه لن يتم المساس بالمنشورات الفردية وكبح حريات المواطن، بل المنشورات التي تروج أخبارا مغلوطة وكاذبة من شأنها المساس بأمن الدولة والمجتمع.

وثمن الرئيس الجزائري عبد المجيد تبون إنشاء القطب المتخصص في الجرائم الإلكترونية، كمكسب لقطاع العدالة على غرار القطب الجزائي المتخصص في مكافحة الجرائم المالية والاقتصادية، مع التشديد على الإسراع في تنصيب القطب الجديد ومعالجة الجرائم الإلكترونية المعروضة حاليا، أمام العدالة.

### 4. تجريم المشرع الجزائري لنشر الأخبار الملفقة:

وفي هذا الصدد يرى الخبير القانوني الجزائري رشيد لوراري " أن هذا النوع من الجرائم الإلكترونية حديث العهد في البلاد في ظل وجود شبه فراغ قانوني لمعالجتها، ومع ذلك يمكن مبدئيا معالجة هذا النوع من القضايا انطلاقا من قانون العقوبات الحالي، مع احترام مجموعة من الحريات والحقوق الأساسية." [1] وتعتبر الأخبار الكاذبة ظاهرة خطيرة يمكن أن تمس بالنظام العام وبأمن واستقرار المجتمع ويمكن أن تمس أيضا بحقوق وحريات الأفراد [2]، فمن الضروري إطلاق ورشة قانونية من الأساتذة والمختصين، للإسراع في إعداد مشروع قانون يغطي الفراغ في التعامل مع مثل هذه القضايا . ومن أجل مواجهة ظاهرة الانتشار المتسارع الأخبار الملفقة قام المشرع الجزائري بتعديل المادة 196 مكرر من قانون العقوبات ينص على معاقبة كل من ينشر أو يروج عمدا بأي وسيلة كانت أخبارا أو أنباء كاذبة أو مُغرضة بين الجمهور من شأنها المساس بالأمن العمومي أو النظام العام، نظرا لما يترتب عن هذه الأفعال من بث الرعب لدى المواطنين وخلق جو من انعدام الأمن في المجتمع". كما ينص هذا التعديل على فرض "عقوبة جنحية على هذه الأفعال تتمثل في الحبس من سنة (1) إلى ثلاث (3) سنوات وغرامة مالية تتراوح بين 100.000 دج الى 300.000 دج".[3]

---

(1)بدون كاتب، 2020/04/28، **الأخبار الكاذبة حول كورونا : كيف تتعامل معها الدول العربية ؟**، http://magazine.maharat-news.com/misinformationandcorona، مجلة مهارات، لبنان، تم الاطلاع عليه بتاريخ 2021/03/12 .

(2) Kuldeep Nagi , **New Social Media and Impact of Fake News on Society** , Assumption University of Thailand , Bangkok , 2019 , p 64 .

(3) الجمهورية الجزائرية الديمقراطية الشعبية، رئاسة الجمهورية، الأمانة العامة للحكومة، الجزء الثاني : التجريم =

## 5. تجريم المشرع الجزائري للتمييز ونشر خطاب الكراهية عبر الفضاء السيبراني

إن الفضاء السيبراني غير مراقب وغير مقيد، سواء في الجزائر أو في العالم العربي، وبالتالي فإن تداول المعلومات يكون سريعا ومنتشرا وغير محدود. كما أن الحسابات الوهمية والمواقع المزيفة وظهور بعض الممارسات التي أفرزتها التكنولوجيا كالذباب الإلكتروني مثلا، يساهم في انتشار خطابات التميز والكراهية والعنصرية... وهناك أيضا بعض الأسباب النفسية والاجتماعية والثقافية ترجع للمرجعيات العرقية والدينية وكذا القومية التي لاقت انتشارا واسعا مع نهاية الحربين العالميتين الأولى والثانية وهجرة العديد من الأجناس إلى أوروبا ما أدى إلى ظهور دعاة العرقية والإثنية وامتدت عبر التاريخ وتبلورت مع مواقع الشبكات الاجتماعية.

ولهذا عملت الدولة الجزائرية، كغيرها من بلدان العالم والمؤسسات الدولية، على تبني مقاربة متعددة الأبعاد في مواجهة المخاطر الكبيرة لخطاب الكراهية، لاسيما في البيئة الرقمية، حيث تم إقرار قانون خاص بجرائم التميز وخطاب الكراهية ومكافحتهما تحت رقم 05.20، فكان لهذا السند القانوني دور أساسي في ضبط مختلف جرائم خطاب الكراهية وهي متعددة الصور وأشكال التعبير، حسب ما جاء في القانون الصادر في الجريدة الرسمية للجمهورية الجزائرية في 28 أفريل 2020.

وفي إطار الإستراتيجية متعددة الأبعاد للحكومة الجزائرية في محاربة التنامي الخطير لظاهرة خطاب الكراهية، لاسيما في الفضاء الرقمي، تم استحداث المرصد الوطني للوقاية من التميز وخطاب الكراهية كآلية جديدة بموجب ما نص عليه القانون 20-05. ويعتبر هذا المرصد، حسب منطوق المادة 10، هيئة وطنية تتولى "رصد ومتابعة كل أشكال ومظاهر التميز وخطاب الكراهية، وتحليلها وكشف أسبابها واقتراح التدابير والإجراءات اللازمة للوقاية منها[1]."

صدر في العدد الأخير من الجريدة الرسمية، القانون رقم 20-05 المؤرخ في 28 أبريل

<الكتاب الثالث : الجنايات والجنح وعقوباتها < الباب الأول : الجنايات والجنح ضد الشيء العمومي < الفصل السادس : الجنايات والجنح ضد الأمن العمومي < القسم الرابع : التسول والتطفل < المادة 196 مكرر، 2020/08/3، ص 76 .

(1) الجمهورية الجزائرية الديمقراطية الشعبية، الجريدة الرسمية، **القانون رقم 20-05 المؤرخ في 28 أبريل 2020، المتعلق بالوقاية من التميز وخطاب الكراهية ومكافحتهما .**

2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، والذي يتضمن إنشاء المرصد الوطني للوقاية من التمييز وخطاب الكراهية.

ويحدد القانون المهام الموكلة لهذا المرصد الذي يوضع لدى رئيس الجمهورية، والمتمثلة في اقتراح عناصر الإستراتيجية الوطنية للوقاية من التمييز وخطاب الكراهية، والمساهمة في تنفيذها بالتنسيق مع السلطات العمومية المختصة ومختلف الفاعلين في هذا المجال والمجتمع المدني، إلى جانب الرصد المبكر لأفعال التمييز وخطاب الكراهية وإخطار الجهات المعنية بذلك.

كما يتولى المرصد تبليغ الجهات القضائية المختصة عن الأفعال التي تصل إلى علمه والتي يحتمل أنها تشكل جريمة من الجرائم المنصوص عليها في هذا القانون، ويتولى أيضا تقديم الآراء أو التوصيات حول أي مسألة تتعلق بالتمييز وخطاب الكراهية.[1]

وحسب المادة 11 من ذات القانون، فإن المرصد الوطني يتشكل من ستة أعضاء من بين الكفاءات الوطنية، يختارهم رئيس الجمهورية ويتم تعيينهم بموجب مرسوم رئاسي لعهدة مدتها 5 سنوات قابلة للتجديد مرة واحدة، ويمثل هؤلاء الأعضاء كل من المجلس الأعلى للغة العربية، المحافظة السامية للأمازيغية، المجلس الوطني لحقوق الإنسان، الهيئة الوطنية لحماية وترقية الطفولة، المجلس الوطني للأشخاص المعوقين وسلطة ضبط السمعي البصري، بالإضافة إلى أربعة ممثلين للجمعيات الناشطة في مجال تدخل المرصد يتم اقتراحهم من الجمعيات التي ينتمون إليها.[2]

## خاتمة:

نستنتج من خلال ما سبق وبعد تحليلنا لهذا الموضوع المتعلق بتأثير الجريمة السيبرانية على الفضاء الاتصالي الجزائري وسبل مواجهتها، نستنتج أن المشرع الجزائري بالرغم من إصداره لمجموعة من التشريعات المقننة للفضاء السيبراني في إطار مواكبة التطور الذي عرفته البشرية في استخدام الوسائل الإلكترونية الحديثة بكثرة من جهة، واقتداء من

---

***(1)*** حميدة نواصرية ( 2022/02/09 )، **لهذه الأسباب انتشر خطاب الكراهية عبر مواقع التواصل**، http://www.ech-chaab.com/ar، تم الإطلاع عليه بتاريخ 2022/11/10 .

(2) الجمهورية الجزائرية الديمقراطية الشعبية، الجريدة الرسمية، **القانون رقم 20-05 المؤرخ في 28 أبريل 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما .**

المشرع الجزائري بباقي التشريعات المقارنة والمواثيق والاتفاقيات الدولية التي صادق عليها المقنن الجزائر في هذا المجال من جهة ثانية.

إلا أن المشرع الجزائري يلاحظ أنه عجز عن مواكبة هذا التحول المعلوماتي أو الثورة الإلكترونية وهو ما يظهر من خلال القرارات القضائية المتضاربة والقليلة بشأن الجرائم الإلكترونية، ولعل ذلك راجع إلى أن النصوص القانونية التي يشوبها نقص وقصور كبيرين سواء من حيث توفير الوسائل الفنية والتقنية الكفيلة بمساعدة القضاء على البت فيها، وكذلك انعدام موارد بشرية مدربة ومكونة في هذا النوع من الجرائم المستحدثة، خصوصا إذا ما أخذنا بعين الاعتبار صعوبة اكتشاف الدليل المعلوماتي. عكس الجريمة التقليدية المرتكبة بوسائل تقليدية، فالإشكال المطروح هو أن العدالة الجنائية، تعمد إلى مواجهة الجريمة السيبرانية المرتكبة بوسائل حديثة بوسائل تقليدية بحتة.

كما يجب على المشرع الجزائري أن لا يخلط بين الجريمة السيبرانية وحرية التعبير والحق في الإعلام والحق في الاتصال، فمهمة المشرع هي تنظيم الفضاء السيبراني والأنشطة الاتصالية في عصر الوسائط الجديدة بدون تضييق أو كبح لمبادئ حقوق الإنسان.

## المراجع:

**المراجع العربية:**

**1.الكتب:**

.عبير شفيق الرحباني، الجرائم الإلكترونية ومخاطرها، دار الثقافة للنشر والتوزيع، الأردن، 2020 .

. محمود عمر محمود ، الجرائم المعلوماتية والإلكترونية بالتطبيق على الهاتف المحمول، خوارزم العلمية، السعودية، 2015 .

. محمد عبد الرحمن عنانزة، القصد الجرمي في الجرائم الالكترونية، دار الأيام للنشر، عمان، 2017 .

.سمير عالية، الجرائم الإلكترونية، منشورات الحلبي الحقوقية، بيروت، 2020 .

.حفوظة الأمير عبد القادر وغرداين حسام، الجريمة الالكترونية وآليات التصدي لها، كتاب أعمال ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري المنعقد في الجزائري العاصمة يوم 29 مارس 2017 .

**2. المراسيم والقوانين:**

- القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات، ج.ر .عدد 71.

- القانون رقم 23/06 المؤرخ في 20 ديسمبر المعدل والمتمم لقانون العقوبات، ج.ر .عدد 84.

- القانون رقم 02/16 المؤرخ في 19 ماي 2016 المعدل والمتمم لقانون العقوبات، ج.ر .عدد 37.

- المادة 45 من القانون رقم 07/17 المؤرخ في 27 مارس 2017 المعدل والمتمم لقانون الإجراءات الجزائية، ج.ر .عدد 20.

- القانون رقم 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج.ر .عدد 47.

- الجمهورية الجزائرية الديمقراطية الشعبية، رئاسة الجمهورية، الأمانة العامة للحكومة، الجزء الثاني: التجريم، الكتاب الثالث: الجنايات والجنح وعقوباتها، الباب الأول: الجنايات والجنح ضد الشيء العمومي، الفصل السادس: الجنايات والجنح ضد الأمن العمومي، القسم الرابع: التسول والتطفل، المادة 196 مكرر، 2020/08/3، ص76.

- الجمهورية الجزائرية الديمقراطية الشعبية، الجريدة الرسمية، القانون رقم 20-05 المؤرخ في 28 أبريل 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما.

- الجمهورية الجزائرية الديمقراطية الشعبية، الجريدة الرسمية، القانون رقم 20-05 المؤرخ في 28 أبريل 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما.

**3.المواقع الإلكترونية:**

- علي ياحي (2022/03/07)، تطوير المنظومة القضائية والأمنية في الجزائر لمواجهة الجرائم المعلوماتية، https://www.independentarabia.com/node/309351/، تم الإطلاع عليه بتاريخ 2022/11/07.

- بدون كاتب، 2020/04/22، إجراءات جزائية جديدة لوضع مروجي الأنباء الكاذبة أمام مسؤولياتهم وسد فراغ قانوني، https://www.aps.dz/ar/algerie/86444-2020-04-22-14-02-04، وكالة الأنباء الجزائرية، تم الاطلاع عليه بتاريخ 2021/03/07 .

- حميدة نواصرية (2022/02/09)، لهذه الأسباب انتشر خطاب الكراهية عبر مواقع التواصل، http: //www.ech-chaab.com/ar، تم الاطلاع عليه بتاريخ 2022/11/10 .

**المراجع الأجنبية:**

-Thomas J. Holt , Cybercrime and Digital Forensics An Introduction , Routledge , usa , 2022.

-Kuldeep Nagi , New Social Media and Impact of Fake News on Society , Assumption University of Thailand , Bangkok , 2019 .